REMARKS

Applicants appreciate the detailed examination evidenced by the Office Action mailed December 11, 2008 (hereinafter "Office Action"). Applicants have amended the specification to delete reference to "a carrier wave embodied in an electrical, electromagnetic, infrared, or optical signal." Applicants submit that these amendments overcome the rejections of Claims 45-52 under 35 U.S.C. §101.

Applicants have also amended independent Claims 29 and 45 to further highlight patentable distinctions over the cited references. In particular, Applicants have amended independent Claims 29 and 45 to clarify that the presence of an anomaly at a first device is detected based on information polled from ***at least two*** devices of a networked computer system. For example, independent Claim 29 now recites:

> A method of anticipating a device in a networked computer system is to be affected by an anomaly, comprising:
>
> polling a plurality of devices of the networked computer system in a predetermined scheduled sequential order for information relating to network communications thereof;
>
> detecting an anomaly occurring at a first device in the computer system ***from information obtained from at least two devices of the polled plurality of devices of the networked computer system*** using network-based intrusion detection techniques comprising analyzing data entering into a plurality of hosts, servers, and computer sites in the networked computer system; and
>
> determining a second device that is anticipated to be affected by the anomaly by using pattern correlations across the plurality of hosts, servers, and computer sites ~~following~~ responsive to the detection of the anomaly and prior to polling of the second device.

Independent Claim 45 has been similarly amended. These amendments represent an incorporation of subject matter related to dependent Claims 34 and 49, which recite anomaly detection based on packets received by at least two devices.

Independent Claims 29 and 45 stand rejected as being allegedly obvious with respect to a combination of U.S. Patent Application Publication No. 2003/0110392 to Aucsmith et al. ("Aucsmith") and U.S. Patent Application Publication No. 2002/0078382 to Sheikh et al. ("Sheikh"). Office Action, p. 3. The Office Action asserts that Aucsmith discloses "detecting an anomaly at a first device in the computer system using network-based intrusion detection techniques comprising analyzing data entering into a plurality of hosts, servers, and computer

sites in the networked computer system [Fig. 1, paragraph 0037-0039, Fig. 2, step 206]." Office Action, p. 3. However, Paragraph [0037] states:

> [0037] When information arrives at the client 102, ***the agent*** 106 examines the information and determines 206 if the information includes or indicates a known anomaly. Known anomalies include security problems that the server 104 has identified to the agent 106 and/or security problems that the agent 106 was initially configured to identify (and that have not since been deleted as anomalies to identify). The agent 106 may make this determination in real time.
>
> [0038] In identifying known anomalies, ***the agent*** 106 may compare the information with information included in a collection of anomalies data included as part of the agent 106, in a collection of anomalies data included in the client 102 or otherwise accessible to the agent 106, in the corporate collection of security data 120, or in another similar resource.
>
> [0039] For example, a packet may arrive at the client 102. ***The agent*** 106 may compare a source Internet Protocol (IP) address included in or with the packet with IP addresses of known intruders included in the corporate collection of security data 120. In another example when a packet arrives at the client 102, the agent 106 may examine the packet for particular queries or commands that fit an intrusion pattern or technique identified in the corporate collection of security data 120.
>
> [0040] ***If the agent 106 does not detect a known anomaly, then the agent 102 returns 208 to waiting for another piece of information to arrive at the client 102 or to examining a piece of information that already arrived at the client 102.*** The client 102 may also process the information as appropriate because the information does not present a known security problem.
>
> [0041] If the agent 106 does detect a known anomaly, then the agent 106 can report 210 the anomaly to the server 104. The agent 106 may report the anomaly in real time. The agent 106 may report the anomaly directly to the server 104 or to the server 104 through a network such as the VPN 114. The agent 106 may not report the anomaly to the server 104 or even know that notice of the anomaly will reach the server 104 but rather report the anomaly to an intermediary, such as to the corporate server 116 via the VPN 114. In this particular example, assume that the agent 106 transmits notice of the anomaly to the server 104 via the VPN 114 and the corporate server 116. (emphasis added)

As can be seen in these paragraphs, in the system of Aucsmith, the agent, which is located at a client device, detects an anomaly at that client ***based only on information received at that client***, and then subsequently informs the server of the detected anomaly. The server described in Aucsmith does not appear to take any actions absent report of a detected

anomaly from the agent. Thus, Aucsmith does not disclose or suggest "detecting an anomaly occurring at a first device in the computer system ***from information obtained from at least two devices of the polled plurality of devices of the networked computer system*** using network-based intrusion detection techniques comprising analyzing data entering into a plurality of hosts, servers, and computer sites in the networked computer system."

The Office Action further concedes that Aucsmith does not teach "polling a plurality of devices of the networked computer system," but asserts that polling described in Sheikh would be an obvious modification of Aucsmith "since one would have been motivated to monitor the computer network systems for security purposes." Office Action, p. 4. The above discussion of Aucsmith, however, illustrates why this reasoning is erroneous. As discussed above, the system of Aucsmith is driven by each ***agent*** independently detecting anomalies. There would have been no reason to modify Aucsmith according to Sheikh to utilize polling multiple ones of such client devices and detection of anomalies by a server based on the polling of the multiple client devices, as the original anomaly detection in Aucsmith is done by the client-based agents, not by the server.

Accordingly, the cited combination of Aucsmith and Sheikh does not disclose or suggest all of the recitations of amended independent Claims 29 and 45, and there is no reason to combine Aucsmith and Sheikh to produce the recitations of these claims. For at least these reasons, Applicants submit that amended independent Claims 29 and 45 are patentable. Applicants submit that dependent Claims 31-35, 43, 44 and 46-52 are patentable at least by virtue of the patentability of the respective ones of independent Claims 29 and 45 from which they depend. Applicants further submit that several of the dependent claims are separately patentable.

As all of the claims are now in condition for allowance, Applicants respectfully request allowance of the claims and passing of the application to issue in due course. Applicants urge the Examiner to contact Applicants' undersigned representative at (919) 854-1400 to resolve any remaining formal issues.

Respectfully submitted,

Robert M. Meeks
Registration No. 40,723
Attorney for Applicants

USPTO Customer No. 39072
Myers Bigel Sibley & Sajovec
Post Office Box 37428
Raleigh, North Carolina 27627
Telephone: 919/854-1400
Facsimile: 919/854-1401

CERTIFICATION OF TRANSMISSION

I hereby certify that this correspondence is being transmitted via the Office electronic filing system in accordance with § 1.6(a)(4) to the U.S. Patent and Trademark Office on April 13, 2009.

Audra Wooten